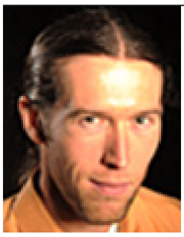
Top 12 Best Practices for Virtualizing Active Directory Domain Controllers



Greg Shields
Microsoft MVP and VMware vExpert

Our industry is evolving towards the reality that every IT workload can now be virtualized.

Services, applications, even high-powered databases have now become virtual machine (VM) candidates thanks to advancements in hardware and hypervisor technology. Yet while all manner of applications find themselves running atop VMs today, doing the same with Active Directory domain controllers (DCs) remains one of IT's greatest questions. You may have wondered yourself,

"Should I virtualize my DCs, and if I do what mistakes could I make?"

The short answer is: *Plenty.*

A DC is unlike other IT workloads in a variety of ways. Its implementation of multi-master replication must be carefully designed to avoid replication errors. Its services require a transactional database that can't be backed up like regular files and folders. Most importantly, its functionality exists as the foundation for every other IT service. Lose Active Directory and you've lost that foundation. Lose objects within it, and the people and computers those objects represent are quickly locked out.

Yet even as DCs are critical to IT operations, they aren't large consumers of server resources. Even an environment of 1,000 users might never see their Active Directory database grow much larger than about 400 megabytes. CPU and memory utilization tend to be relatively small as well. That same 1,000-user organization might only need a dual processor server with a gigabyte or two of RAM to operate with good performance.

The issue, however, is the fact that Active Directory domain controllers—at a minimum—come in pairs. Due to geographic distances, many environments find themselves needing even more. It isn't unheard of for a widely-distributed organization to need tens or dozens of DCs to serve the authentication needs of clients. For what is a relatively lightweight service, Active Directory on a physical server represents a cost that seems easy to cut through virtualization.

12 Best Practices You must not Miss

What causes those virtual activities to suddenly switch from easy to difficult? The answer lies in complexity. Managing a VMware vSphere environment is at first a simple task: Install ESX(i), power on VMs, monitor their performance, ensure they've got the resources they need. Yet working with that virtual infrastructure grows geometrically more challenging as your number of hosts and VMs increases.

More hardware adds more interdependencies. More VMs require more hardware. More business activities generate more VMs. As a result, maintaining the highest levels of server consolidation and best performance quickly becomes an activity no human alive can accomplish unaided.

Contrary to what you may think, virtualizing DCs isn't an activity to be entered into lightly. While virtualization indeed brings benefits, it also adds risk when virtualized DCs are not created smartly. Thankfully, our industry is beginning to agree on a set of intelligent recommendations that ensure the health and security of virtualized DCs. If you're considering virtualization for your Active Directory DCs, or even if you've virtualized them already, don't miss these 12 important best practices.

Neglecting the advice of any could kill your entire computing infrastructure.

Best Practice #1: DCs Require VM High Availability

The DCs that power Active Directory are a marvel of high availability. Leveraging multi-master replication not often seen in database applications, Active Directory is by itself a remarkably resilient service. It has to be. With every part of a Windows infrastructure requiring Active Directory's authentication services, those services must remain highly-available.

With that high-availability, however, comes an expectation that DCs are nearly always operational. Active Directory itself goes as far as disabling disk write caches on volumes hosting its database and log files. This action helps to preserve the integrity of the database should the server unexpectedly go down.

Even so, preventing DC outages must be a priority. *Any virtualized DCs should be hosted in a highly-available virtual environment.* Clustering virtual hosts together enables that environment to quickly fail a VM to a new host when problems occur, getting that DC back online in short order. It is not a good practice to virtualize a DC onto a host that lacks a VM-level high availability infrastructure.

Best Practice #2: Never Pause, Never Clone, Never Snapshot… Except…

Virtualization at first blush appears to add a wide range of new capabilities for virtual servers. Once virtualized, a server's state can be paused in addition to being powered on and off. Its disks can be snapshotted and/or cloned in order to protect their contents or duplicate them elsewhere.

These hypervisor snapshotting, pausing, and cloning capabilities are functions of the virtual platform that powers your VMs. They can be excellent tactics in the virtual administrator's quiver of administrative solutions for many kinds of servers. *However, using any of them in this fashion against a DC is never recommended.*

Reverting to a previous VM snapshot of a DC effectively rolls that server backward in time. It also rolls the DC's database backward, which represents a behavior that Active Directory's multi-master replication was never designed to handle. Database corruption, USN rollback, and replication problems are only a few of the nasty results that can occur. Similar problems can surface should a virtualized DC get paused for too long a time.

Cloning DC disks introduces another series of issues entirely, and should be avoided at all times. When a DC detects that its disk signature has changed, a situation which can occur with cloning, the DC will isolate itself from multi-master replication. The DC may appear to function, but other DCs are no longer replicating with it. Over time this situation creates a divergence between the contents of the isolated DC and others. Users with deleted accounts might still be granted logon access. Others with newly-created accounts may experience unpredictable results. Avoid all of these problems by avoiding cloning entirely.

This guide for "never snapshotting" has one important caveat. Some data protection solutions are able to provide full application-aware quiescence during a snapshot. This quiescence prevents the data corruption problems that can occur with unassisted hypervisor snapshots. So, never snapshot…unless your VMs enjoy the assistance of such a data protection solution

Best Practice #3:
Not All Backups Are Created Equal

Virtual platform snapshotting and cloning are activities one should never attempt against a DC. That said, the terms "snapshot" and "clone" sometimes have other meanings outside the virtual platform, such as in the case of some backup solutions. Even Microsoft's built-in Volume Shadow Copy Service uses similar terms to describe backup and restore processes that are, in fact, good ideas for DC backups.

That's why the third best practice in this list suggests educating yourself on all the backup options available for DCs. The backup solution you want is one that gathers the necessary data quickly via an image-based, block-level approach. Doing so provides near-continuous data protection while exposing the full range of single item restoration all the way through an entire forest recovery.

You won't get that with Microsoft's native tools alone. Microsoft's tools for backing up Active Directory were never built with user-friendliness in mind. Restoring individual objects is difficult. Restoring entire DCs requires a multistep process fraught with risk. Attempting to resurrect a corrupted forest is a task in which even the most experienced IT administrator won't succeed without help.

The right solution will enable you to restore any object, server, or forest back to any period in time. That period of time might be "yesterday," or it might be "15 minutes ago" depending on your recovery requirements.

Best Practice #4:
Avoid Clock Drift

Keeping clocks properly synchronized is a task that's not terribly difficult on physical servers. Once synchronized, a physical server's clock will remain at the correct time for a long while. The same does not hold true in virtual environments. Due to the irregular patterns of attention a VM gets from its hypervisor, clock drift is an issue requiring constant attention.

Clock drift in a VM can be handled by the virtual platform's installed tools, or it can be handled by synchronizing clocks to an external time source. Pick one, and use it for every virtual DC you deploy. No matter which option you choose, pay careful attention to your DC's clocks. Should their clocks drift beyond a mere five minutes, you'll find your DCs will no longer service client requests.

Best Practice #5: Don't Overprovision Resources

When prototypical IT pros build a DC atop a physical server they often find themselves using a standard configuration. "Dual cores and four gigs of RAM" is a common mantra you'll hear from administrators. That level of processing power and memory makes sense when DCs are on physical hardware. The cost differential between one gigabyte and four gigabytes of RAM is often less than the time required to engineer the correct quantity.

Virtual environments are much different. Even with the resource overcommitment capabilities built into hypervisors today, assigning too many resources to a VM is still an unnecessary waste. Host resources are required to manage the overcommitment, and VMs with unnecessarily large resource commitments can complicate load balancing activities.

Don't make your virtual environment work harder than it needs. *Use performance management tools to find and assign the right quantity the VM needs, and avoid assigning multiple virtual processors whenever possible.*

Best Practice #6: Ensure Backups Actually Work

Foolish is the IT pro who focuses too exclusively on backups; wise is the IT pro who recognizes restorability is the ultimate goal. Even referring to this class of software as "backup solutions" obscures the reality that a backup isn't usable unless it can be verifiably restored.

The right solution for protecting your Active Directory data will not only backup and restore that data, it will also automatically verify the integrity of each backup. You want a solution that performs an integrity check for every backup on your behalf. That verification gives you the guarantee that every object, DC, or forest restore will complete successfully.

Best Practice #7: Implement Anti-Affinity Rules

VMs are constantly moving around their virtual environment. The always-changing nature of server resource utilization means that load balancing is a never-ending activity. But while relocating VMs is great for keeping the balance, it also introduces the possibility that two DCs could end up collocated on the same host. That collocation is a situation you want to avoid.

Every virtual platform comes equipped with a unique implementation of what are generically called "affinity rules." Affinity rules enable an administrator to determine which VMs should always, and which should never, end up on the same host as a result of load balancing relocations. *An anti-affinity rule is important with any virtualized DCs. That rule will instruct the virtual environment to ensure DCs never end up on the same host.* Separating those DCs ensures that the loss of a host won't cause an entire Active Directory outage.

Best Practice #8: Separate Client and Administrator Traffic

The red button one clicks to power off a VM is no different than the power button on a physical server. Hit that button, either physically or virtually, and the VM along with its workload are going to go down.

Power operations, snapshotting, cloning, and migrating represent activities that are performed within a virtual platform's management console. They also represent actions to which regular users must never have access. You lock the doors of your datacenter, limiting access to a privileged few. You should do the same with your virtual infrastructure. *Separating client network traffic from the traffic used for virtual environment activities is just as important as locking your datacenter.* Doing so protects the important buttons, the virtual ones in this case, from accidentally (or maliciously) being clicked.

Best Practice #9: Prioritize Quick Object Restores

Until the release of Windows Server 2008 R2, Active Directory was not equipped to handle individual object restores. Even after its release, the native Active Directory Recycle Bin remains a challenge to work with. Complex PowerShell operations are required to gather data and restore deleted objects. Even finding the right object to restore is difficult, particularly when speed is of the essence.

It is for this reason why every DC, virtualized or not, should be protected using solutions that prioritize quick restores. Virtualization can provide an assist with this process. For example, a virtualized DC can be resurrected to a protected location for the purpose of restoring data. Once restored, the DC can be safely removed without impacting the production environment.

Seek an Active Directory backup solution that restores deleted objects with minimum time and effort. You'll enjoy making it home for dinner the next time an Organizational Unit full of objects finds itself accidentally deleted.

Best Practice #10: Monitor Storage Performance

In virtualization's early days, processing and memory were considered two of the biggest bottlenecks to acceptable performance. Getting enough processing power to needy VMs at that time was a priority for every virtual administrator.

Today we find that storage has become a primary source of performance loss. That performance loss can come from incorrectly-configured or oversubscribed connections. It can result from overtaxing SAN disks or spindle contention. *While virtualized DCs tend not to have heavy storage performance requirements, monitoring IOPS (input/output operations per second) across storage connections is important to performance management.* Even though your DCs might not require the fastest disks in the world, the activities of other hosts and VMs can create problems. Only by monitoring storage behaviors can those impacting activities be located and resolved.

Best Practice #11: Remain a Bit Physical

Even with the benefits virtualization brings to servers, your virtual environment itself could be a single point of failure. Hypervisor vulnerabilities, storage interruptions, and resource overutilization are all extreme scenarios that could result in a virtual environment-wide outage.

That outage becomes even more problematic when the entirety of your Active Directory resides in the failed virtual environment. Often, fixing the outage starts by fixing directory services. If directory services can't be made available, resolving the problem becomes a significantly more challenging process.

Returning a failed virtual environment to operations requires the same Active Directory foundation your servers need while they're in operations. *Thus, preserving at least one DC as a physical server will ensure your Active Directory foundation remains, even during the worst of virtual environment outages.*

Best Practice #12: Have a Plan Solution for Disaster Recovery

Preparing for the worst requires having more than just a plan for disaster recovery. It also requires the solutions that enable executing that plan. *Incorporating the tools for backing up Active Directory data is only part of the plan. Regularly ensuring that your tools are functioning and can resurrect servers and data is what fulfills your solution.*

You won't get there with native backups alone. Windows' native system state backup will indeed capture a copy of Active Directory data, but it does so in a manner that's not easily restorable after the disaster occurs. That's not a functioning solution.

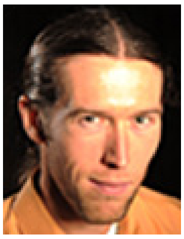
A solution that works is one that restores entire DCs (as well as other servers) in minutes rather than days, quickly resurrecting your environment to get business back online. Look for solutions that can restore the functionality of virtual machines without the long delay required in physically restoring its data. At the end of the day, what you need is a functioning Active Directory. The right solution will bring those services online quickly, while transparently finishing the long, slow restore in the background.

Virtualize DCs with Care.
Protect Their Data with Greater Care.

Making the decision to virtualize your Active Directory DCs can be smart for datacenter operations. Doing so frees server resources for other activities. It also adds the high availability and migration features every virtual server enjoys. But while virtualizing those DCs can make your life easier, doing it incorrectly will have the opposite effect down the road. These 12 best practices should get you started toward the right configuration and design.

A major portion of that design includes finding the right solutions for protecting Active Directory's data. As the foundation of your entire datacenter, protecting data requires extreme care. Be smart about how you virtualize your DCs. Be even smarter about how you protect their data.

About the Author



Greg Shields, Microsoft MVP and VMware vExpert, is an independent author, speaker, and IT consultant, as well as a Partner and Principal Technologist with Concentrated Technology. With 15 years in information technology, Greg has developed extensive experience in systems administration, engineering, and architecture specializing in Microsoft OS, remote application, systems management, and virtualization technologies.

About Veeam Software

Veeam Software, an Elite VMware Technology Alliance Partner, develops innovative software to manage VMware vSphere®. Veeam vPower™ provides advanced Virtualization-Powered Data Protection™ and is the underlying technology in Veeam Backup & Replication™, the #1 virtualization backup solution. Veeam nworks extends enterprise monitoring to VMware and includes the nworks Management Pack™ for VMware management in Microsoft System Center and the nworks Smart Plug-in™ for VMware management in HP Operations Manager. Veeam ONE™ provides a single solution to optimize the performance, configuration and utilization of VMware environments and includes: Veeam Monitor™ for easy-to-deploy VMware monitoring; Veeam Reporter™ for VMware capacity planning, change management, and reporting and chargeback; and Veeam Business View™ for VMware business service management and categorization. Learn more about Veeam Software by visiting www.veeam.com.